Abstraction qualitative et surveillance de systèmes cyber-physiques

Baptiste Gueuziec[1], Jean-Pierre Gallois[1], and Frédéric Boulanger[2]

[1] Université Paris-Saclay, CEA, LIST, F-91120 Palaiseau, France
baptiste.gueuziec@cea.fr, jean-pierre.gallois@cea.fr
[2] Université Paris-Saclay, CNRS, CentraleSupélec
Laboratoire Méthodes Formelles, Gif-sur-Yvette, France
frederic.boulanger@centralesupelec.fr

Résumé

La surveillance de systèmes cyber-physiques en temps réel est une activité industrielle primordiale nécessitant de déployer des ressources, notamment en termes de capteurs, de traitement de signal, ainsi que d'analyse des informations obtenues. De fait, le choix du nombre de ces capteurs et de leur fréquence d'échantillonnage est un compromis entre la consommation de ressources et le niveau de sûreté.

Le principe de la surveillance du système est d'utiliser les informations fournies par les capteurs pour calculer à chaque instant la position de l'état du système dans l'arbre de ses comportements théoriques, afin de détecter les évènements anormaux et d'anticiper leurs conséquences. Cependant, cette méthode offre peu d'outils pour optimiser ce processus.

En utilisant l'abstraction et la modélisation qualitative, nous proposons une méthode permettant d'obtenir une carte qualitative de l'espace d'états du système, et d'utiliser celle-ci afin d'optimiser le choix des instants de mesure et des calculs à effectuer, pour améliorer l'efficacité de la surveillance des systèmes cyber-physiques en temps réel.

1 Introduction

Les systèmes cyber-physiques constituent une classe d'objets assez vaste dont la complexité, la nature et la susceptibilité aux erreurs sont très variables. La partie physique de ces systèmes est en général décrite par des modèles continus tandis que le système complet avec son contrôleur sera décrit par un modèle hybride [10], car il exhibe des comportements continus et discrets. Afin que le système réel soit le plus fiable possible, de nombreux travaux sont effectués en amont pour anticiper ses propriétés, ses risques de défaillance, ses possibles déviations au fonctionnement de référence et sa résilience aux fautes. Cela nécessite d'employer des méthodes de test ou de diagnostic [15, 18], ou, quand cela est possible, de preuve formelle [16]. Ces dernières, utilisant très souvent des langages de preuve symbolique, se combinent assez bien avec le paradigme dit de modélisation qualitative, permettant de visualiser l'arbre complet des comportements qualitatifs que le système pourra adopter.

Définition : Un système est dit hybride s'il implique à la fois des comportements continus et discrets. De tels systèmes peuvent être représentés par :

— Un ensemble Q de variables discrètes définissant le mode du système,
— Un ensemble X de variables continues.

Nous nous intéressons plus spécifiquement à l'étude et à la surveillance d'un système pouvant se représenter par $S = \langle Q, X, F, I, T \rangle$, avec Q le vecteur de l'ensemble des variables discrètes du système évoluant sur l'espace discret $\mathbf{D}_Q$, X l'ensemble des variables continues du système évoluant sur $\mathbb{K}^n$ (avec par défaut $\mathbb{K} = \mathbb{R}$ et $n = card(X)$) tel que $\forall (m, x) \in \mathbf{D}_Q * \mathbb{K}^n$, (q, x) représente l'état du système, F la dynamique du système représentée par des équations de

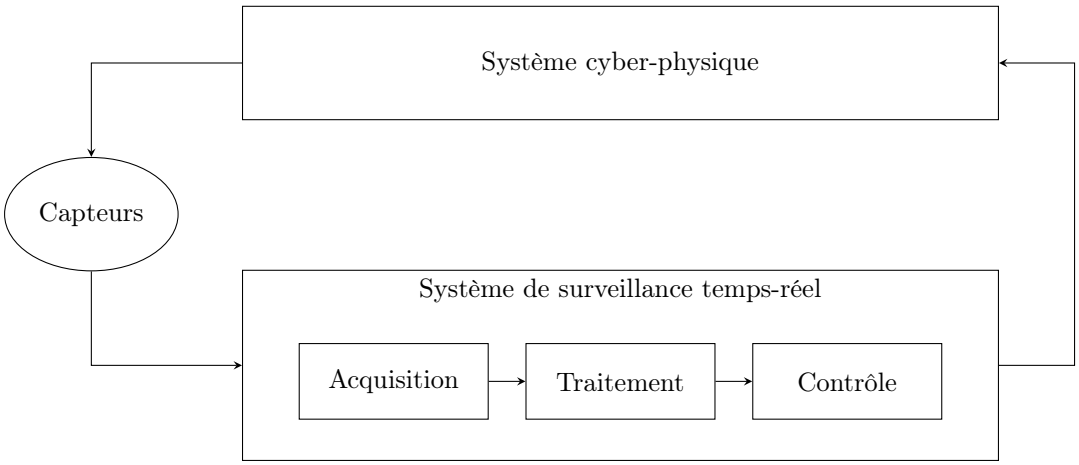

FIGURE 1 – Cycle surveillance et contrôle en temps réel d'un système cyber-physique

dépendance directe ou des équations différentielles ordinaires, I l'ensemble des invariants du système sous la forme d'inégalités sur ses variables, que l'on considère comme des contraintes inviolables, et T l'ensemble des transitions modales du système, représentées sous la forme de quadruplets $(m_1 \in \mathbf{D}_Q, cond \in 2^{\mathbb{K}^n}, m_2 \in \mathbf{D}_Q)$, f qui correspond au changement de la valeur discrète $Q = m_1$ vers $Q = m_2$ lorsque la condition $cond$ est vérifiée avec réinitialisation de x à $f(x)$. La surveillance en temps réel du système de la Figure 1 implique d'observer l'évolution du comportement de celui-ci via l'intermédiaire de capteurs, de traiter le signal relevé par ceux-ci afin d'en obtenir une information exploitable et d'utiliser cette information afin de s'assurer du bon déroulement du processus physique ou au contraire d'appliquer une correction. Il est donc nécessaire de pouvoir agir en retour sur le système en fonction du résultat de l'échantillonnage. Dans cet article, nous avons choisi de nous concentrer principalement sur la problématique du choix et de la qualité de l'échantillonnage ainsi que sur les informations à tirer de cette mesure. Le but recherché est d'optimiser les ressources dépensées dans l'utilisation des capteurs disponibles et de maximiser l'efficacité de la détection de tout comportement déviant. Nous souhaitons également qu'aucune déviation violant les invariants du système ne puisse avoir lieu avant d'être détectée. Les problématiques liées au traitement du signal et à la correction du système ne seront pas traitées ici. Cet article correspond à un prolongement de nos travaux sur le raisonnement qualitatif appliqué à la simulation de systèmes complexes [7, 8] pour une application de ceux-ci à la surveillance.

2 Modélisation Qualitative

2.1 Bases du raisonnement qualitatif

Le paradigme dit de modélisation qualitative a vu le jour lorsque Brown [3] et De Kleer [5] ont élaboré et publié une représentation abstraite, dite qualitative, des connaissances disponibles sur un système. Ces connaissances incluent les dépendances entre les éléments, leurs dynamiques respectives ou encore l'ensemble des causalités associées. A l'origine, cette forme de représentation était particulièrement utilisée pour résoudre des problèmes de physique, d'électronique et pour aider à la résolution de problèmes généraux par ordinateur. Jusque dans les années

90, les méthodes et les idées de raisonnement qualitatif se sont diversifiées et complétées grâce aux apports de nombreux informaticiens, notamment Forbus [6], Hayes [9], et Kuipers [13]. Ces contributions ont notamment apporté au domaine des réflexions sur la fermeture conceptuelle, les graphes de concept et les équations différentielles qualitatives. Cependant, en dépit de ces apports, la discipline de la modélisation qualitative restait assez abstraite et ne permettait que peu de choses sur les systèmes comportant des boucles de rétroaction, ou au comportement trop complexe.

Ces obstacles ont été franchis grâce aux travaux effectués plus tard notamment par Berleant et Kuipers sur le paradigme dit semi-qualitatif [1], par les travaux sur le diagnostic de systèmes dynamiques de Mosterman [15] ainsi que par ceux de Tiwari sur l'abstraction de systèmes dynamiques définis par des équations différentielles ordinaires [17]. Ces dernières contributions ont très largement permis à la modélisation qualitative de devenir ce qu'elle est aujourd'hui, et d'y associer des possibilités telles que la propagation d'intervalles et d'incertitude, le diagnostic, ou encore la création de l'arbre de comportement exhaustif de certains systèmes. En général, on peut définir la modélisation qualitative comme une représentation du système ne s'intéressant pas à la valeur précise de ses variables voire de ses paramètres, mais en considérant seulement leur position par rapport à certaines valeurs spécifiques [14]. Cependant, la gestion des variables considérées ainsi que de leurs valeurs n'est pas la même en fonction de la méthode considérée. Dans les modèles les plus simples, on s'intéresse seulement aux variables explicitement déclarées dans le système, qu'on compare uniquement à 0. Autrement dit, on s'intéresse à leur signe et on raisonne donc sur l'algèbre des signes, générée par le triplet de valeurs $(+, -, 0)$. Certaines méthodes, comme celle que propose Kuipers, se sont intéressées à la possibilité de considérer d'autres valeurs de référence, appelées landmarks, tandis que le modèle de Tiwari s'intéresse plutôt à la création de nouvelles variables pour le système, en utilisant notamment ses polynômes et leurs dérivées.

De fait, en introduisant l'ensemble P des polynômes du système définis sur $\mathbb{K}[(X_i)_{0<i\leq n}]$ (contenant par exemple l'expression des équations différentielles ordinaires, des barrières déduites des invariants de I et conditions de garde des transitions modales exprimées dans T) et de leurs dérivées jusqu'à l'ordre d (la valeur de d pouvant être spécifiée en amont ou non), on peut alors utiliser tous les éléments de P comme nouvelles variables du système dont on étudiera le signe. Il est par ailleurs à noter que cette méthodologie se généralise assez bien à l'ensemble des fractions rationnelles, dont le signe du numérateur et du dénominateur peuvent alors être étudiés séparément. Les nouvelles variables obtenues avec P sont alors ajoutées à celles de X dans un nouvel ensemble des variables étendues X_p. Les zéros de toutes ces variables dérivées sont alors calculés par des solveurs adaptés, et leur expression est associée à une frontière dans l'espace d'état, qu'on appelle frontière qualitative. Passer une de ces frontières revient à changer d'état qualitatif, et donc à changer la valeur abstraite de X. Ce processus s'appelle l'abstraction de l'espace d'états de S. Il détermine un ensemble d'états qualitatifs qui correspondent chacun à un domaine de l'espace d'état concret du système. Il permet à tout instant d'associer à une valeur spécifique de l'état du système un unique état qualitatif représenté par le signe des éléments de X_p à cet instant.

2.2 Calcul de l'arbre des comportements

Une fois l'espace des états qualitatifs déterminé, il est possible de s'intéresser aux transitions d'un état qualitatif à un autre. Cela peut se faire en utilisant la dérivée de Lie : lorsqu'on étudie une frontière entre deux états, et que cette frontière correspond à l'annulation de la variable étendue x_p, pour savoir dans quel sens la transition est possible, il faut se placer sur un point

s de cette frontière. En calculant la dérivée de Lie, de formule $L_X(x_p) = \sum_{x \in X} \frac{\partial x_p}{\partial x} \frac{dx}{dt}$ en ce point, on peut déterminer en fonction du signe du résultat dans quel sens il est possible d'aller. En répétant le processus pour tous les états et en effectuant une exploration de l'arbre des états en s'arrêtant sur la branche courante lorsqu'on trouve un état déjà visité, on peut alors obtenir un arbre complet des comportements qualitatifs du système dans son mode de fonctionnement normal. À moins d'un dysfonctionnement ou d'une intervention extérieure, toutes les trajectoires numériques du système seront incluses dans ces routes générales.

2.3 Ajout de valeurs exogènes au système

La méthode de discrétisation de l'espace d'états que nous venons de présenter a l'avantage majeur d'être très générale et d'être facilement applicable à un grand nombre de systèmes, y compris partiellement instanciés puisqu'elle ne prend en compte que les paramètres internes du système sans s'intéresser à leur contexte ou a leur application. Cet avantage peut cependant devenir gênant lorsqu'on veut s'intéresser à des systèmes intégrés à leur milieu, combinés à d'autres systèmes ou tout simplement utilisés pour une tâche spécifique. Ce qu'on veut alors permettre est la prise en compte par notre modèle de contraintes concrètes, proches de l'expertise métier. On a donc choisi pour cela de créer une nouvelle structure de système dérivée de celle déjà présentée : à tous les éléments déjà introduits, on ajoute les ensembles C et O de $2^{\mathbb{K}^n}$, correspondant respectivement aux spécifications métiers associées au système et aux objectifs de celui-ci. On perd alors beaucoup en généralité sur le modèle obtenu mais les conclusions qu'on pourra en retirer seront plus adaptées et spécifiques.

Ces nouvelles équations ajoutées au modèle sont alors considérées comme de nouvelles variables dérivées, comme celles présentées plus tôt. Cela nous permet de fixer des seuils à surveiller, dont le dépassement ne correspond pas à une erreur mais à une augmentation substantielle des risques que cela advienne. Par exemple, si on étudie un système clos contenant de l'eau liquide, et qu'on s'intéresse à la stabilité du système associée à un invariant sur la pression de celle-ci, l'augmentation de la température à 100 degrés constitue non pas une contrainte stricte à ne pas franchir, mais bien un indicateur de plus forte probabilité que la contrainte soit ensuite violée. Cet indicateur nous permet déjà de réfléchir par minimisation du risque : si on sait qualitativement qu'un tel seuil a été franchi, on sait que les probabilités de survenue d'un comportement dangereux ont augmenté. Il semble donc cohérent d'augmenter la fréquence d'échantillonnage des capteurs associés à la variable ayant dépassé le seuil et à celles présentant un risque de fausse conduite tant que l'estimation du risque n'aura pas retrouvé son niveau d'avant franchissement. Ainsi, on utilise de manière plus optimisée les capteurs dont on dispose, en fonction de l'état qualitatif courant, lorsque ceux-ci induisent des connaissances pertinentes sur les objectifs et risques du système. Cependant, nous pouvons aller plus loins plus loin en exploitant le raisonnement qualitatif pour optimiser d'avantage leur utilisation.

3 Zones qualitatives et cartographie de l'espace d'états

Notre principal apport en terme d'évolution de la modélisation qualitative a consisté à augmenter la connaissance disponible à tout moment sur l'état courant du système, sans perdre l'avantage de l'abstraction. Comme la méthode de discrétisation en états qualitatifs a déjà fait ses preuves, nous nous sommes d'avantage concentrés sur la création d'un nouveau type de structure discrète qui puisse compléter les états qualitatifs sans les remplacer. Les états qualitatifs contenant et donnant de l'information sur le signe des différentes variables et équations du système, nous avons voulu trouver une manière d'intégrer dans la représentation qualitative du

système une abstraction de la distance d'un point aux différentes frontières séparant les états qualitatifs. L'information de cette valeur a une réelle importance sur le plan pratique : si on sait qu'on se trouve à proximité (selon un critère qu'il reste cependant à définir) d'une transition qualitative voir modale du système à un moment donné, il est judicieux d'adapter la stratégie de gestion des capteurs pour anticiper le changement de comportement du système.

3.1 Création des zones qualitatives

Pour commencer, il nous faut définir cette notion de zone qualitative. Soit S un système cyber-physique tel que défini plus tôt. On suppose qu'on a pu appliquer la méthode d'abstraction en états qualitatifs et qu'on dispose de l'arbre des comportements qualitatifs de S. On connaît donc, pour chaque état qualitatif q_s de S l'ensemble de ses successeurs et on peut en déduire l'ensemble de ses prédécesseurs. L'ensemble fini des états qualitatifs du système est noté Q_s. On obtient alors un ensemble B de frontières séparant ces états qualitatifs entre eux. On mémorise également la nature de chaque frontière (*landmark*, équation d'ordre supérieur, ou équation de dynamique), car de cela dépendra la création de la zone associée.

Nous cherchons alors à définir des frontières secondaires, entourant et délimitant la proximité dans l'espace d'état des éléments de B, qu'on appellera par contraste frontières principales. La proximité doit cependant être définie selon des critères précis. Dans le cas des landmarks (définis comme des hyperplans par l'équation $X_i = d$ avec $0 < i < n$, X_i la i^{e} composante de X et d une constante), on mesure trivialement la proximité avec la distance euclidienne, calculée par soustraction des équations porteuses des hyperplans : on définit donc les frontières secondaires comme des hyperplans parallèles à la frontière qualitative principale et translatés de d et $-d$ selon l'axe de X_i, avec d une valeur à définir en amont. Pour les frontières définies par des égalités moins triviales (notamment celles obtenues avec les équations d'évolution dynamique), on se contente de transférer la distance des variables d'origine aux variables dérivées : les frontières secondaires seront donc de la forme $x_p = \pm d$ pour tout x_p variable étendue de X. Se pose alors le problème du choix de ces valeurs de d.

Dans le cas des landmarks, comme les valeurs sont associées aux variables principales du système, les valeurs à choisir rejoignent la réflexion menée sur les variables exogènes du système : en regardant quelles valeurs pour chaque composante de X ont un intérêt particulier pour l'analyse du système (on va ici s'intéresser au taux de franchissement, et donc aux valeurs de d qui vont induire un taux de dépassement des frontières de l'état courant supérieur à une valeur donnée), on peut choisir des valeurs de d qui offrent une certaine marge de manœuvre mais qui garantissent une haute probabilité de transition. Un tel compromis permet alors de créer une zone dite d'intérêt, lorsque le système se situe entre la frontière principale et une de ses frontières secondaires. La présence du système dans cette zone spécifique nous renseigne alors sur l'imminence et la probabilité des prochaines transitions, ce qui est utile dans le cadre de notre supervision. De la même manière, le choix d'une distance d pour les équations plus complexes hors équations de dynamique dépendra d'une analyse préalable des probabilités de franchissement de la frontière en cas de pénétration dans la zone ainsi définie.

L'étude de la probabilité pourra alors se faire selon un tirage de Monte-Carlo sur un nombre d'échantillons suffisants afin d'obtenir un résultat significatif. Enfin, dans le cadre des équations de dynamique, le choix de la distance se fait comme précédemment sur la distance euclidienne par rapport à la variable dérivée, ce qui ne correspond à priori à aucune distance strictement définie dans l'espace porté par X. Dans ce cas précis, tracer les frontières déduites de l'égalité de ces équations à une constante revient à tracer les isoclines des différentes composantes de X. Dans ce cas, il est difficile d'anticiper la forme que prendra la frontière secondaire puisqu'elle

n'est pas directement calculée dans l'espace d'états.

De plus, comme nous l'avons étudié dans nos précédents travaux, l'utilisation de multiples isoclines (courbes définies pour une variable y par $\dot{y} = c$ avec c une constante) permet en plus de quantifier non seulement la distance à une transition qualitative, mais également de connaître une abstraction de la vitesse de variation des variables. Or, plus une variable évolue rapidement, plus le système est susceptible de commettre des mouvements extrêmes, et de brusquement franchir une frontière ou de dévier de son comportement initial. Ainsi, il est pertinent d'utiliser à la fois des isoclines de faible valeur pour indiquer la proximité d'une nullcline (courbe définie pour une variable y par $\dot{y} = 0$) et donc d'une transition, mais également des isoclines de valeurs plus importantes pour anticiper des comportements à évolution rapide et à fort risque de transition imprévue. Les premières correspondent à des dérivées faibles en valeur absolues, tandis que les secondes correspondent à des dérivées de valeurs absolues élevées. Cette double information sera d'autant plus utile lorsqu'une des composante de X sera faible en norme alors qu'une autre sera élevée, car la seconde pourra entraîner des conséquences disproportionnées sur l'évolution de la première.

3.2 Superposition des couches d'informations

La création de zones qualitatives ne se substitue pas à l'utilisation des états qualitatifs précédemment présentés, mais elle s'y ajoute. De fait, l'utilisation des états qualitatifs offre principalement des informations sur la dynamique du système [17, 18]. A l'inverse, les zones peuvent compléter ces états qualitatifs en ajoutant une notion de distance à la frontière des états. Mais les zones seules ne permettent pas l'étude de la dynamique en raison de la méconnaissance des signes car elles chevauchent les frontières entre états qualitatifs.

L'arbre des comportements présenté en subsection 2.2 permet par exemple d'identifier les comportements cycliques entre états qualitatifs, mais ne permet pas de déterminer si ce cycle converge vers un état stable. Grâce aux zones qualitatives, on peut déterminer cette convergence en considérant une boule de rayon ε centrée sur l'hypothétique point de convergence, et en utilisant la dérivée de Lie pour savoir si on peut entrer ou sortir de cette boule.

De plus, l'algèbre des signes, utilisée pour l'étude des états qualitatifs, est beaucoup plus permissive en termes d'opérations que toute autre abstraction de l'espace d'état d'un système [14], il faut donc pouvoir l'utiliser seule, tout en conservant la possibilité d'y ajouter les informations apportées par les zones. Une algèbre plus complexe qui prendrait en compte les deux notions en même temps serait inutilisable dans certains cas.

Une fois la carte établie, il est alors temps de l'exploiter au mieux afin d'optimiser l'utilisation prévue du système (ici la surveillance en temps réel).

On définit un système d'oscillateur de Van der Pol avec les équations suivantes :

$$\begin{cases} \dot{x} = 10(y + x - \frac{x^3}{3}) \\ \dot{y} = b - x - \frac{3y}{4} \end{cases} \tag{1}$$

avec b une constante. La Figure 2 montre un exemple de carte qualitative obtenue pour un oscillateur de Van der Pol en superposant une discrétisation en états qualitatifs utilisant le calcul des zéros des équations du système pour tracer les frontières principales (en traits pleins sur la représentation), ainsi que le calcul des zones qualitatives pour les frontières secondaires (en pointillés). Les premières ont donc été obtenues par résolution et tracé des équations $x = 0, y = 0, \dot{x} = 0$ et $\dot{y} = 0$. Les frontières secondaires (dont la couleur correspond aux frontières qualitatives associées), sont obtenues en résolvant les mêmes équations en remplaçant 0 par $\pm c$, avec ici $c = 0.2$.

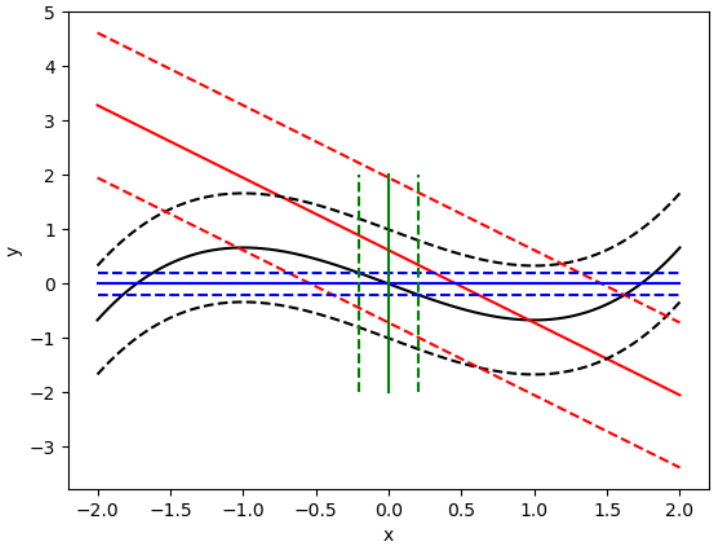

FIGURE 2 – Exemple de carte qualitative

Cette représentation unifiée possède de nombreuses caractéristiques en commun avec une carte de reliefs de type IGN, où les frontières principales seraient les lignes de crête et les frontières secondaires seraient des courbes de dénivelé ou des courbes de sommets intermédiaires plus bas que les premiers. En utilisant comme évoqué des courbes secondaires multiples, on peut alors avoir une cartographie en plusieurs dimensions de l'espace d'états du système. De plus, en dérivant à plusieurs reprises les équations de la dynamique pour affiner la discrétisation de l'espace d'états [17], on peut fonder le choix du nombre de dérivations effectuées sur la quantité d'information que l'on veut que cette carte contienne.

4 Lecture de la carte et surveillance du système

4.1 Anticipation des zones à risque

La mise en place de la carte qualitative dans la partie précédente nous permet maintenant de définir ce qu'on considère comme des zones d'intérêt, ou des zones critiques. Tout d'abord, les zones de proximité des différentes frontières principales de l'espace d'état constituent un bon exemple de ce que l'on considère comme une zone critique : la proximité d'une frontière implique la possible survenue prochaine d'une transition (qu'elle soit modale ou intra-modale), que l'on veut en général détecter pour adapter le tracé de référence puisque le comportement va évoluer après celle-ci. Quand on fait de la simulation en amont de l'exécution et qu'on n'a pas la contrainte du temps réel, on peut se permettre de repérer précisément l'instant d'apparition de la transition en effectuant du rollback [2], ou en appliquant des méthodes de propagation de domaine plus élaborées [11, 4]. Cet artifice ne nous est malheureusement pas permis dans le cadre de la surveillance temps réel : si un événement que l'on voulait détecter a déjà eu lieu, il est trop tard. Ainsi, on va chercher à anticiper les problèmes plutôt qu'à les résoudre. C'est ici que se justifie notre proposition d'utiliser la carte qualitative pour adapter le pas d'échantillonnage en fonction de la zone qualitative courante du système.

4.2 Adaptation du pas d'échantillonnage

Si on appelle position qualitative le couple (qs, qz) avec qs l'état qualitatif courant du système et qz l'ensemble des zones qualitatives qui le caractérisent, alors qs va nous informer des prochaines transitions et violations de contraintes possibles, tandis que qz va expliciter les principaux risques et ceux qui sont le plus susceptibles de se produire à court terme. Cette information est pertinente pour l'adaptation de notre fréquence d'échantillonnage : on va traduire l'intérêt qu'on porte à une zone critique ou d'intérêt par le biais d'un facteur numérique k qu'on appellera facteur de criticité. Plus la zone courante est considérée comme critique ou importante, plus la valeur de k sera élevée. On fait de choix de considérer $k \in \mathbb{N}$ et $k_{ref} = 1$ la valeur de référence lorsque la zone courante n'a aucun intérêt ou risque particulier. Lorsqu'on entre dans des zones plus importantes pour l'étude du système, k devra alors être augmenté. De plus, la fréquence d'échantillonnage des capteurs devra être modifiée en conséquence. Plus la position courante est proche d'une barrière d'invariant ou d'une transition discrète, plus on va augmenter cette fréquence pour être certain de maximiser la précision de la localisation de l'événement. La valeur de k devra donc être augmentée dans ces zones.

De façon moins intuitive en revanche, la superposition de plusieurs zones considérées critiques n'est pas additive. Au contraire, il arrive même qu'elle soit dégressive. Dans le cas d'un système S à deux variables x et y, si les dérivées des deux variables sont proches de l'annulation et qu'on est dans l'intersection de leur zone de criticité, on sera certes proche de deux transitions simultanément, mais la faible valeur des dérivées implique que le système ne variera que peu dans les prochains instants, ce qui retardera celles-ci. À l'inverse, la proximité d'une seule nullcline réduit le nombre des prochaines transitions disponibles, mais la valeur inconnue de la dérivée de la variable non concernée implique une incertitude sur l'amplitude des variations à venir. Si celles-ci s'avèrent importantes, la transition considérée pourra alors être franchie beaucoup plus vite que dans le cas précédent. La relation générale entre nombre d'intersection de zones critiques et augmentation de la valeur courante de k n'est donc pas triviale, et est trop contextuelle pour en donner une règle générale.

Ce que nous avons remarqué empiriquement est que la superposition de deux zones de même nature n'entraîne pas de modification notable du niveau de criticité. Ainsi, nous allons considérer qu'en cas d'intersection entre plusieurs zones, $k_{intersection} = \max(k_z)$. En revanche, la criticité d'une zone augmente avec la valeur des dérivées des composantes de la variable du système. Ainsi, comme on a dans la partie précédente tracé les isoclines de proximité, on voit maintenant le besoin de les associer à leurs homologues pour les valeurs élevées des dérivées : lorsque la valeur des dérivées est importante, il est judicieux de prendre plus de précaution pour éviter les transitions intempestives.

Ces nouvelles zones doivent cependant être considérées différemment des précédentes : bien qu'ici encore, il ne soit pas utile de considérer les intersections entre zones de dérivée importante, la superposition de zones de natures différentes aura cette fois un effet additif sur la valeur de k dans la zone née de l'intersection. En effet, lorsqu'une des variables possède une importante vitesse de variation et qu'une autre se trouve à proximité de sa nullcline, l'influence de la première sera d'autant plus importante que la deuxième ne pourra la compenser. On a ainsi pour chaque fragment de l'espace d'état une valeur de k. Il s'agit maintenant de traduire celle-ci sous forme de fréquence d'échantillonnage.

Une façon simple de procéder est de transformer ce facteur en fréquence par une multiplication : si on a estimé à k le facteur de criticité, on peut alors définir la période d'échantillonnage associée par b/k, avec b la base dans laquelle on va travailler et qui correspond à la période d'échantillonnage de référence, lorsque $k = 1$. Cette valeur de k va donc dépendre du système sur lequel on travaille et des applications qu'on va rechercher. Il est nécessaire de définir celle-ci

en amont de l'exécution du système, puisque cette valeur servira véritablement de base de calcul pour la suite.

Ainsi, à toute position qualitative du système (q_s, q_z) sera associée une fréquence d'échantillonnage appliquée aux capteurs de S d'une valeur de k/b, selon les notations déjà définies.

4.3 Qualité des mesures et quantification du système

L'une des difficultés majeures de l'application du raisonnement qualitatif au domaine de la prévision, du diagnostic et de la simulation de systèmes est la perte d'information sur l'état du système au cours de l'exécution du modèle. En effet, une fois des valeurs numériques abstraites en état qualitatif, il est extrêmement complexe de revenir à une valeur numérique précise lorsqu'on le souhaite. Ce qui s'en rapproche le plus est la fonction dite de concrétisation [17], qui transforme l'état qualitatif courant en ensemble numérique à partir des contraintes définissant celui-ci. On est cependant loin de pouvoir précisément situer le système dans son espace d'états à tout instant. De plus, les possibles successeurs multiples d'un état qualitatif ajoutent une incertitude encore supérieure à la situation actuelle du système. Vu sous cet angle, la gestion de systèmes en temps réel semble être un excellent domaine d'application pour le raisonnement qualitatif puisque l'utilisation de capteurs et le gain d'information permettent précisément de corriger cette lacune fondamentale.

En effet, lorsqu'il est nécessaire d'augmenter la connaissance disponible sur l'état du système, ou de connaître la trajectoire qualitative empruntée pour un état à successeurs multiples, il suffit d'exiger de nouvelles mesures des capteurs de surveillance. Ainsi, la fonction de concrétisation β du système revient simplement à l'appel aux capteurs pour effectuer une nouvelle mesure. Ainsi, nous avons fait le choix de rendre la précision des mesures (notamment en termes de décimales des valeurs) fonction de la valeur de k de la zone courante. Cela permet de nouveau d'optimiser des ressources de calcul lorsque le système n'a que peu de chances de rencontrer une situation dangereuse, tout en ne sacrifiant pas la précision lorsqu'elle est nécessaire puisque l'information peut être ré-obtenue à tout moment. Elle le sera d'ailleurs lorsqu'on entrera dans les zones les plus critiques puisque lorsque la présence dans une telle zone sera connue, cela sera précisément grâce à un échantillonnage de l'état du système qui le situera dans une position digne d'intérêt. Cette possibilité de connaître à tout moment la position numérique du système permet également de jouer avec la précision des mesures et d'optimiser la complexité des calculs effectués. On peut effectivement opter pour une grille de quantification des états numériques qui sera, comme le pas de temps, variable au cours de l'exécution du système. On se rapproche ainsi de l'étude des systèmes à états quantifiés (QSS) [12, 19], dont les concepts se rapprochent d'ailleurs de ceux du raisonnement qualitatif. Il serait d'ailleurs possible, en suivant cette piste, de désynchroniser les variables du système afin de proposer des mesures adaptées à chacune d'elle séparément. Cela nécessite l'utilisation de plusieurs facteurs de criticité en parallèle, et de les réunir en une variable K de même dimension que X. Algorithmiquement, comme on a imposé $k \in \mathbb{N}$, on peut par exemple imposer que la précision des relevés en termes de décimales soit acceptée à la k^{e} décimale. Cela ne peut cependant pas être universel et dépendra principalement des valeurs rencontrées par ce système et dans son contexte d'utilisation spécifique. Pour être plus général, nous avons choisi de limiter la précision des mesures à 1% de la valeur de chaque variable lorsque la zone n'est ni intéressante ni critique, et de considérer la plus haute précision possible dans le cas contraire.

4.4 Critères d'arrêt du système

Notre surveillance se voulant automatisée, il nous faut définir à l'avance des critères d'arrêt afin de stopper le système lorsqu'il sort de son cadre de fonctionnement anticipé.

On peut pour cela identifier des critères qualitatifs et quantitatifs. Les premiers sont les plus simples à définir puisqu'ils découlent directement de la définition de notre modèle qualitatif du système : si un invariant est violé, ou si une transition (modale ou qualitative) non prévue se produit. Les transitions autorisées étant stockées dans l'arbre des comportements et les invariants étant spécifiés dans l'instance du système étudié, ce sont des conditions qui sont très pratiques à vérifier grâce à notre modèle qualitatif. Pour cela, à chaque mesure des capteurs, on fait appel à la fonction d'abstraction de notre système qui situe l'état courant dans l'ensemble des états qualitatifs et des parties de l'espace interdites par les invariants. On compare également cette abstraction avec celle de la mesure précédente afin de savoir si une transition (qu'elle soit modale ou qualitative) a eu lieu. Si c'est le cas, il faut vérifier que la transition effectuée se situe bien dans l'arbre de comportements qualitatifs calculé en amont. Si l'abstraction du résultat correspond à un interdit ou que la transition passée n'est pas dans ce qu'on s'attendait à obtenir, c'est que le système est sorti de son comportement attendu, et qu'il y a eu dysfonctionnement. Il est donc nécessaire de l'arrêter afin d'éviter tout risque supplémentaire.

L'autre critère d'arrêt qu'il est possible de définir est cette fois d'avantage numérique et consiste à comparer la valeur courante de l'état du système à des valeurs de référence obtenues en amont par des simulations numériques ou par propagation d'intervalles ou de flow-pipe [2, 4]. On s'écarte cette fois du raisonnement qualitatif pour revenir à des considérations plus numériques, mais celles-ci s'emboîtent assez bien avec l'adaptation du pas d'échantillonnage. En effet, c'est principalement dans les zones critiques de l'espace d'état et notamment les zones à forte variation que les déviations par rapport à la trajectoire de référence ont le plus de chance d'apparaître. Il est alors nécessaire de fixer un seuil d'erreur autorisé, soit via une distance maximale à la trajectoire théorique, soit par la nécessité d'inclure la valeur courante de l'état du système dans un rectangle autour de la trajectoire simulée. Cette dernière option est particulièrement intéressante car elle offre la possibilité d'adapter facilement la marge d'erreur à la situation : dans les zones critiques, il sera pertinent de réduire la taille de l'erreur autorisée. Cela sort cependant du cadre de nos travaux et relève d'avantage du domaine de la simulation numérique. L'inclusion d'un critère d'arrêt numérique simple rentrant pleinement dans le cadre de notre projet, une telle clause sera intégrée à nos différents modèles de test.

5 Mise en application

Afin de tester la pertinence de notre production, nous avons appliqué une implémentation de notre modèle sur différents systèmes simples, continus et hybrides, dont nous avons à chaque fois calculé l'arbre des comportements théoriques en amont. On a par exemple pris parmi nos exemple un oscillateur de Van der Pol défini par : $S_{VdP} = <$

$$
\begin{aligned}
Q &= \{\}, \\
X &= \{x, y\}, \\
\mathbf{X} &= \mathbb{R}^2, \\
I &= \emptyset, \\
F &= \{\dot{x} = 10(y + x - \tfrac{x^3}{3});\ \dot{y} = y + (c - x - \tfrac{3y}{4})\} \\
T &= I = \emptyset
\end{aligned}
$$

$>$ (avec x et y définis sur $\mathbb{R}$ et c une constante réelle) et un système chimique hybride

Algorithm 1 Surveillance de l'exécution du système

```
i = initialTime
while i < T_end do
  X_{i+step} = NextState(X_i, step)
  if ViolateInv(X_i) then
    Return Error
  end if
  Q_i = Abstract(X_i)
  Q_{i+step} = Abstract(X_{i+step})
  if Not AllowedTransition(Q_i, Q_{i+step}) then
    Return Error
  end if
  i+ = step
end while
```

(le Brusselator), défini par $S_{Br} = < Q = \{m\},\ X = \{x, y\},\ F = \{m = m_1 : \{\dot{x} = 1 - (b_1 + 1)x + a_1x^2y;\ \dot{y} = b_1x - a_1x^2y\},\ m = m2 : \{\dot{x} = 1 - (b_2 + 1)x + a_2x^2y;\ \dot{y} = b_2x - a_2x^2y\}\},\ I = \{x > 0, y > 0\},\ T = \{(m_1,\ x < y,\ m_2),\ (m_2,\ y < x,\ m_1)\} >$ (avec $m \in \{m_1, m_2\},\ a_1, a_2, b_1, b_2$ des constantes réelles positives et x, y définies sur $\mathbb{R}^+$). Les systèmes choisis sont encore relativement simples et il est prévu de généraliser nos études sur des cas de figure plus complexes avec des sources et des manifestations d'erreur plus nombreuses. Ensuite, nous avons émulé les trajectoires précises de ces systèmes via une simulation numérique très fine. Cela constitue des trajectoires de référence qu'on considère comme les comportements idéaux. Nous avons également émulé plusieurs trajectoires erronées dont la déviation apparaît selon une loi de probabilité exponentielle (afin de représenter la durée de vie des systèmes) et suivant différentes déviations, déterministes ou aléatoires. On considère alors un comportement erroné défini comme $\dot{X} = f(X, t) + d$ avec d le terme de déviation. On a fixé plusieurs valeurs de paramètres et de point de départ, identiques pour les tests des différents systèmes de surveillance. On a notamment choisi ces différentes valeurs de manière à pouvoir observer les différents types de comportements de ces systèmes (cycles stables ou convergeants). Certaines de ces déviations sont légères, afin de représenter le phénomène d'usure et de déviation progressive (simulées ici par l'ajout d'un terme parasite dans les équations différentielles de valeur constante mais aléatoire), et d'autres plus brutales, afin de représenter des situations de rupture instantanée d'un composant du système (qu'on recréé avec la suppression d'un des termes des équations de dynamique).

L'implémentation de nos modèles a été effectuée en langage *Python*, à l'aide de la librairie *Sympy*. Tout d'abord, la première discrétisation de ces systèmes est obtenue par calcul de $x = 0, y = 0, \dot{x} = 0, \dot{y} = 0$ pour les deux systèmes, auxquels on ajoute $x = y$ pour le Brusselator hybride (équation correspondant à la condition de changement de mode). Les cartes qualitatives sont ensuite complétées par calcul des frontières des zones qualitatives, avec les équations $eq = \pm c_d$ avec $eq \in \{x,\ y,\ \dot{x},\ \dot{y},\ x - y\}$ et $c_d = 0.2$ une constante dont la valeur est fixée dans l'ordre de grandeur des valeurs prises par le système. Tous ces calculs sont effectués grâces aux méthodes présentes dans *Sympy* qui permettent une résolution d'égalités avec plusieurs paramètres symboliques. On obtient alors l'expression des variables choisies en fonction des autres, permettant l'obtention des expression des nullclines et hyperplans. Il en est de même pour les isoclines du modèle, calculées avec les mêmes méthodes. Le calcul des transitions entre états et zones qualitatifs, est quant à lui effectué en utilisant le solveur SMT *Z3*, permettant de

Table 1 – Comparaison de résultats pour le Brusselator Hybride

Type de surveillance	Fine	Adaptative	Moyennée	Grossière
Délai de détection d'une erreur (ua)	1.1	1.8	4.3	6.7
Mesures nécessaires	30	22	12	7

Table 2 – Comparaison de résultats pour l'oscillateur de Van der Pol

Type de surveillance	Fine	Adaptative	Moyennée	Grossière
Délai de détection d'une erreur (ua)	0.7	1.2	1.2	4
Mesures nécessaires	25	18	11	7

s'affranchir des limites de *Sympy* sur le calcul des inégalités symboliques [8].

Ces cartes qualitatives sont alors utilisées par le système de surveillance des systèmes pour automatiser la fréquence et la précision des mesures physiques.

Les calculs de la trajectoire de référence et des trajectoires réelles sont effectués en utilisant une méthode de Runge-Kutta avec la bibliothèque *Numpy* et utilisant les fonctions de *Random* pour ce qui est de déterminer l'apparition de la déviation. Si k est le facteur de criticité défini dans section 4 avec k_i celui de la zone i et p la période d'échantillonnage par défaut du système de surveillance, on adapte la période d'échantillonnage dans la zone qualitative i à $p_i = \frac{p}{k_i}$. De même, la précision considérée lors des mesures effectuées par les capteurs disponibles sera choisie à la k^{e} décimale.

Lors de chaque mesure, l'écart à la trajectoire idéale sera mesuré ainsi que l'état qualitatif correspondant à la mesure effectuée (utilisant donc la fonction d'abstraction et la carte qualitative déduite du modèle théorique). Nous considérons qu'une déviation à la trajectoire théorique est détectée lorsque les données récoltées sur la trajectoire réelle impliquent une transition qui n'est pas autorisée par le calcul des dérivées de Lie, ou un des invariants du système est violé. Nous comparons alors notre surveillance adaptative de ces systèmes virtuels avec des surveillances automatisées mais régulières afin d'en tester la pertinence. Nous avons choisi de baser nos comparaisons sur deux critères principaux pour chaque système : le délais avec lequel la déviation est notifiée (ce qui est possible dans le cas d'un système émulé puisqu'on peut enregistrer l'instant où commence le changement de comportement), ce qui démontrera ainsi une plus ou moins grande réactivité du système de surveillance, ainsi que le nombre d'échantillons de mesure effectués pour arriver à ce résultat (ce qui permettra de juger notre capacité à optimiser l'utilisation des ressources). Une surveillance optimale repérera donc une déviation à un instant t très proche de son apparition et avec un nombre de mesures m très faible. Cette comparaison s'effectue à chaque fois sur une vingtaine d'itérations afin de lisser les effets de l'aléatoire et d'obtenir des résultats moyennés, et sur des cas particuliers afin de repérer quelles situations entraînent des difficultés pour chaque type de surveillance.

Les méthodes de surveillance nous servant de témoin ont été choisies respectivement avec des pas d'échantillonnage t_e très fins et très large. Ces deux valeurs de période de mesure correspondent respectivement à la période initiale (donc maximale) et à la période minimale qu'on pourra avoir dans notre système adaptatif, afin de bien mettre en évidence l'avantage d'adapter le pas d'échantillonnage à la position. Nous avons également fait un test similaire avec des valeurs de t_e moyennées, pour compléter l'étude. Dans nos différentes valeurs de pas de temps, on place la valeur de pas large environ 5 fois supérieure à la valeur la plus faible.

On se place dans le cas de simulations suffisamment longues pour que l'observation des comportements de convergence ait un sens et que les divergences soient observables.

Sur les différents systèmes que nous avons étudiés, le résultat principal est qu'avec notre surveillance adaptative, nous obtenons des précisions moyennes nettement supérieures à celles obtenues par les pas de temps fixes élevés et médians. Dans le cas du Brusselator par exemple, les délais de détections exprimés en unité arbitraire ainsi que le nombre de mesures nécessaires à la détection sont représentés dans la Table 1. On observe qu'on obtient, par rapport à la surveillance fine, un gain de ressources assez important, pour une précision bien supérieure à ce que peuvent offrir des surveillances classiques avec le même nombre de mesures. L'étude sur l'oscillateur de Van der Pol nous donne des résultats similaires représentés dans la Table 2. Nous obtenons donc une meilleure utilisation des ressources que dans le cadre de la surveillance naïve, tout en obtenant des résultats proches d'une surveillance fine bien que moins précis. Cela permet de prétendre à une certaine stabilité de performance tout en augmentant l'autonomie du système qui nécessitera alors moins de réglage sur les paramètres de surveillance à appliquer.

Lorsqu'on étudie des situations particulières, on constate que les superviseurs naïf auront tendance à repérer les franchissements de frontières et déviations légères trop tard par rapport à notre système adaptatif. En revanche, ce constat est faux pour l'apparition de cassures brutales : celles-ci posent plus problème à un système qui n'est pas en permanence sur ses gardes qu'à un superviseur constamment vigilant. Notre proposition est donc particulièrement appropriée pour la détection d'évènements non désirés mais se heurte aux limites de l'anticipation par raisonnement qualitatif. Comme ce cas de figure implique par définition des changements de comportements imprévisibles en amont et trop brusques pour y réagir immédiatement, l'adaptation du pas de temps en fonction des comportements qualitatifs anticipés n'a ici que peu d'intérêt et ne permet pas d'améliorer les performances des systèmes de surveillance. On constate donc bien l'intérêt d'appliquer le raisonnement qualitatif pour l'étude des évènements et pour la surveillance du bon déroulement d'un processus.

6 Conclusion

On a donc pu voir que l'utilisation du raisonnement qualitatif permet d'exploiter les connaissances acquises sur le comportement d'un système grâce à l'analyse de son modèle discrétisé afin d'améliorer les capacités de surveillance de son exécution en temps réel. Cette amélioration passe par l'ajout d'une capacité d'adaptation de la fréquence d'échantillonnage et de la qualité des mesures effectuées par les capteurs intégrés au système, afin d'optimiser leur utilisation dans le contrôle de l'exécution. C'est la possibilité de faire une mesure de l'état réel du système qui nous permet de redonner de la précision à l'algorithme de surveillance lorsqu'on s'approche d'une frontière qualitative, ce qui n'est pas possible dans le cas d'une simulation. Le contexte de la surveillance temps-réel est donc bien adapté à notre approche semi-qualitative.

Comme nos tests l'ont montré, cette capacité d'adaptation permet d'observer une réelle amélioration des résultats selon les métriques choisies (nombre de mesures effectuées et délai de détection des erreurs) par rapport à des méthodes de détection automatisées naïves dans le cas des déviations dites qualitatives (donc des transitions imprévues et/ou interdites). Les déviations continues légères sont également bien détectées bien que de façon moins flagrante que les déviations qualitatives. Enfin, les ruptures brutales sont quant-à-elles assez mal détectées par notre méthodologie. Cela pourrait être amélioré en ajoutant des éléments d'étude des composants individuels qui s'ajouteraient à la vision systémique actuellement utilisée. Par exemple, l'introduction de concepts de maintenance prédictive à l'analyse du système et de ses comportements pourrait permettre d'améliorer grandement la détection de ces cassures qui sont encore trop mal anticipées.

Références

[1] Daniel Berleant and Benjamin J Kuipers. Qualitative and quantitative simulation : bridging the gap. *Artificial Intelligence*, 95(2) :215–255, 1997.

[2] Olivier Bouissou, Alexandre Chapoutot, and Samuel Mimram. Computing flowpipe of nonlinear hybrid systems with numerical methods. *arXiv preprint arXiv :1306.2305*, 2013.

[3] Allen L Brown. *Qualitative knowledge, causal reasoning, and the localization of failures*. MIT Artificial Intelligence Laboratory, 1974.

[4] Xin Chen, Erika Abraham, and Sriram Sankaranarayanan. Taylor model flowpipe construction for non-linear hybrid systems. In *2012 IEEE 33rd Real-Time Systems Symposium*, pages 183–192. IEEE, 2012.

[5] J. De Kleer. *Qualitative and Quantitative Knowledge in Classical Mechanics*. AI-TR-. Massachusetts Institute of Technology, Artificial Intelligence Laboratory, 1975.

[6] Kenneth D Forbus. Qualitative process theory. *Artificial intelligence*, 24(1-3) :85–168, 1984.

[7] Baptiste Gueuziec, Jean-Pierre Gallois, and Frédéric Boulanger. Qualitative models for the supervision of cps simulations. In *Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems : Companion Proceedings*, pages 612–616, 2022.

[8] Baptiste Gueuziec, Jean-Pierre Gallois, and Frédéric Boulanger. Qualitative reasoning and cyber-physical systems : abstraction, modeling, and optimized simulation. In *MoDeVVa 2023-20th workshop on model driven engineering, verification and validation*, 2023.

[9] Patrick J Hayes. *Readings in qualitative reasoning about physical systems*, chapter The second naive physics manifesto, pages 46–63. Morgan Kaufmann, 1985.

[10] Thomas A Henzinger. The theory of hybrid automata. In *Verification of digital and hybrid systems*, pages 265–292. Springer, 2000.

[11] Jawher Jerray. Orbitador : A tool to analyze the stability of periodical dynamical systems. In *ARCH@ ADHS*, pages 176–183, 2021.

[12] Ernesto Kofman and Sergio Junco. Quantized-state systems : a devs approach for continuous system simulation. *Transactions of The Society for Modeling and Simulation International*, 18(3) :123–132, 2001.

[13] Benjamin Kuipers. Qualitative simulation. *Artificial intelligence*, 29(3) :289–338, 1986.

[14] Philippe Dague Louise Travé-Massuyès. *Modèles et raisonnements qualitatifs*. Hermes, 10 2003.

[15] Pieter J Mosterman and Gautam Biswas. Diagnosis of continuous valued systems in transient operating regions. *IEEE Transactions on Systems, Man, and Cybernetics-Part A : Systems and Humans*, 29(6) :554–565, 1999.

[16] Yuvaraj Selvaraj, Wolfgang Ahrendt, and Martin Fabian. Formal development of safe automated driving using differential dynamic logic, 2022.

[17] Ashish Tiwari and Gaurav Khanna. Series of abstractions for hybrid automata. In *International Workshop on Hybrid Systems : Computation and Control*, pages 465–478. Springer, 2002.

[18] Hadi Zaatiti. *Modélisation et simulation qualitative de systemes hybrides*. PhD thesis, Université Paris-Saclay (ComUE), 2018.

[19] Jing Zhou, Changyun Wen, Wei Wang, and Fan Yang. Adaptive backstepping control of nonlinear uncertain systems with quantized states. *IEEE Transactions on Automatic Control*, 64(11) :4756–4763, 2019.